CKN Webinar: 2019-03-05

Trusted Platforms for Critical Infrastructure

Rahul Mavila, Product Manager, IOS XR Security

Dan Backman, Portfolio Architect, SP Automation (Security and Cloud Services)

Speakers

Rahul Mavila
Product Manager, SP Security
Cisco

Dan Backman
Platform Architect, SP Automation
Cisco

Securing Today's Service Provider Networks

1. Security and Trust
2. Trust: Enforcement and Reporting
3. Operationalizing Trusted Platform Technologies

Critical Infrastructure Requires Trusted Service Provider Networks

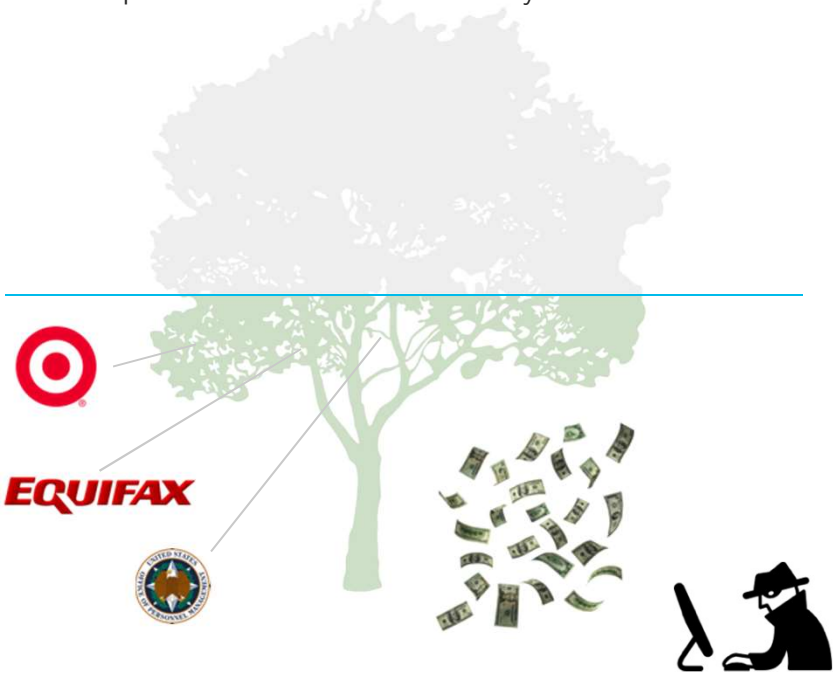
Service Provider Threat Landscape

What Is Trust and Why Does It Matter?

External Validation Services

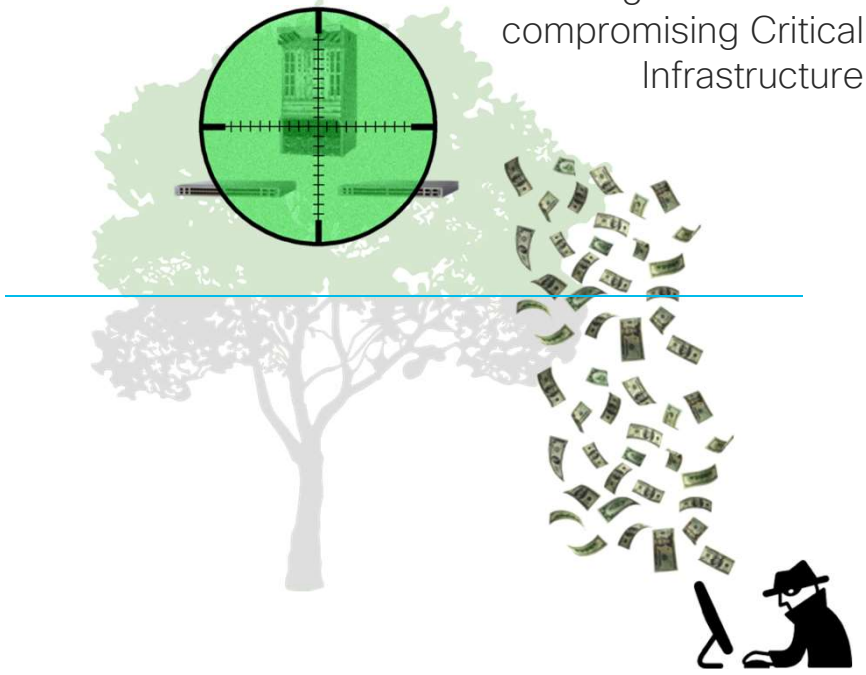
Threat Landscape

Enterprises attacks are mostly robberies



Goal: Exfiltration

Attacking SPs is about compromising Critical Infrastructure



Goal: Turn network into an asset

“Pwning” Critical Infrastructure

- Denial of Service
- Steering of traffic for surveillance
- Introduce MiTM attacks
  - Malicious DNS Services
  - Compromise trusted services (email or SMS)
- Compromise Telemetry

Threat: Long term compromise to leverage network as an asset

What Is Trust and Why Does It Matter?

To build a trusted platform, network infrastructure must be constructed on a platform of trusted technologies to ensure devices operating are authentic and can create verifiable evidence that they have not been altered

Secure
Can never be proven and is an ideal state (a goal)

Trust
Can be measured, verified and audited

Security in IOS XR

Protect the IOS XR OS and Platform

XR Trusted Platform and OS Defenses

IOS XR as Trusted Platform for Critical Infrastructure

Protocol and Platform Hardening

Protocol Security, Control of external threat surface

Securing the IOS XR Threat Surface

IOS XR Security Services

DDoS Protection, Encryption, and New Revenue Services

IOS XR as a delivery platform for security services

Trusted Platform

"Integrity, not just security."

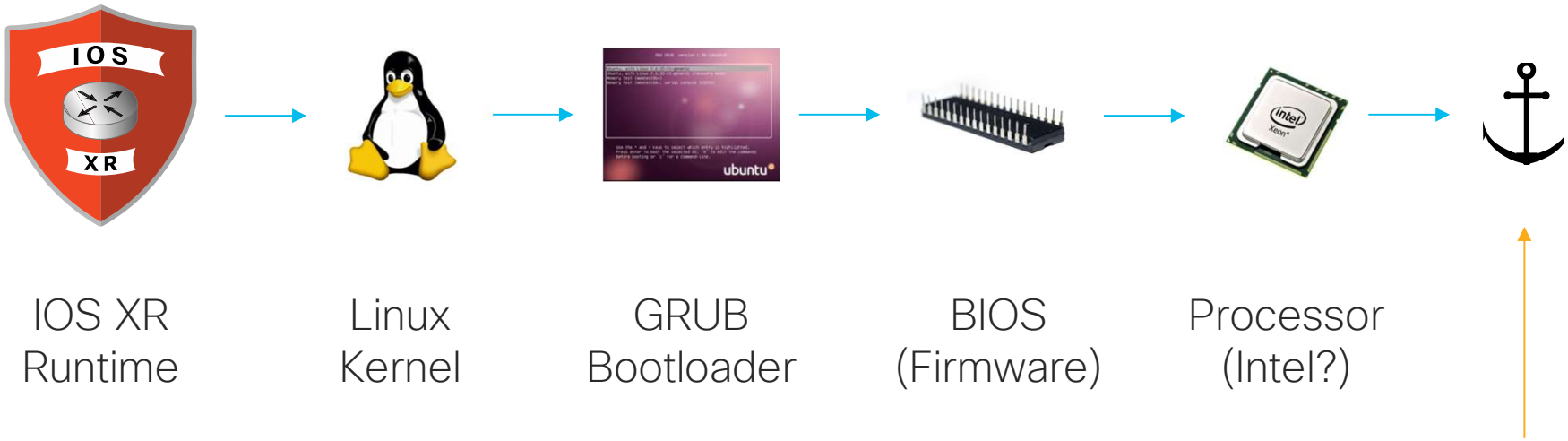
But first, let’s talk a bit about trust & security…

Two primary concepts

Security Controls

Tamper Evidence

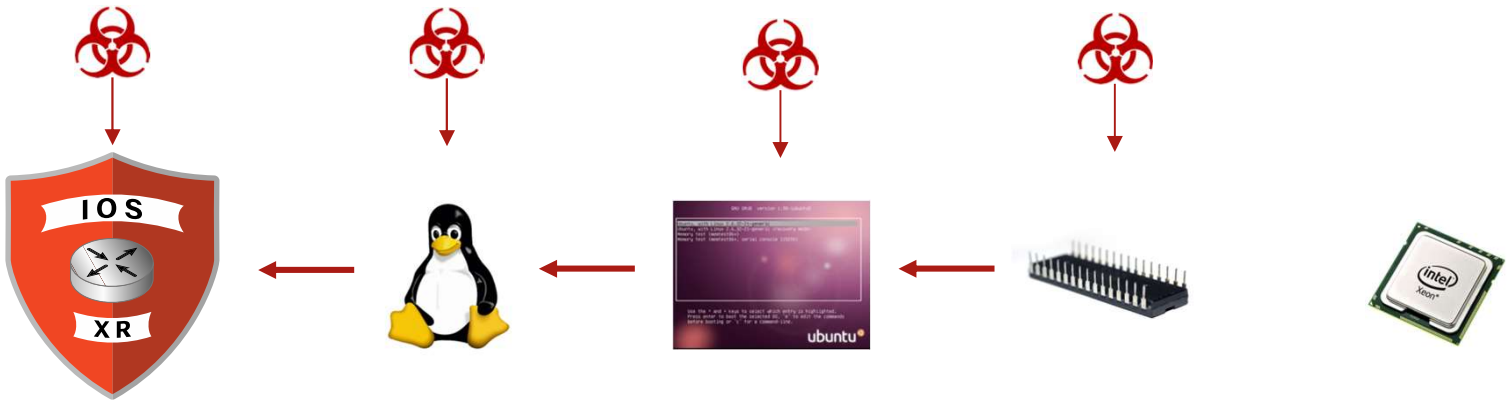
Chain of Trust



IOS XR Runtime → Linux Kernel → GRUB Bootloader → BIOS (Firmware) → Processor (Intel?) → ⚓

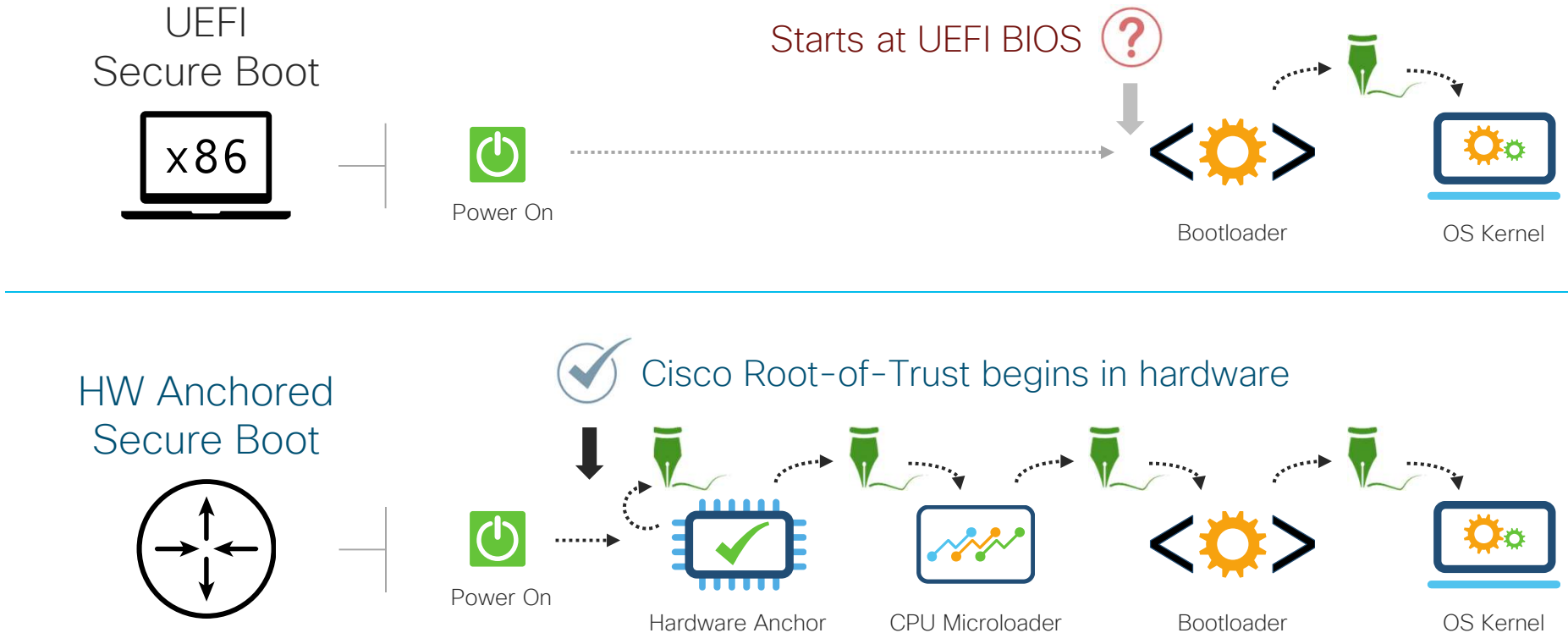
Root-of-Trust (Trust Anchor)

Attacking System Integrity

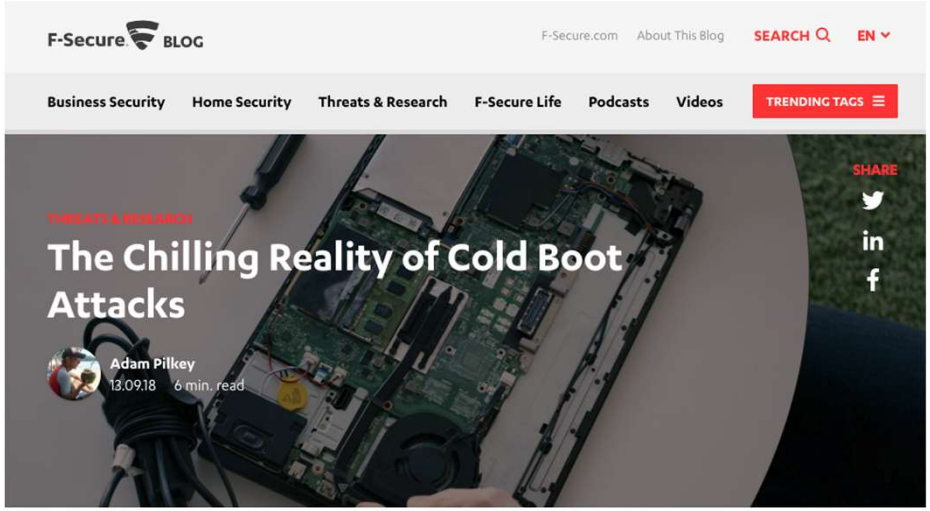


IOS XR Runtime | Linux Kernel | GRUB Bootloader | BIOS (Firmware) | Processor (Intel?)

Cisco Secure Boot vs Standard x86 Solutions



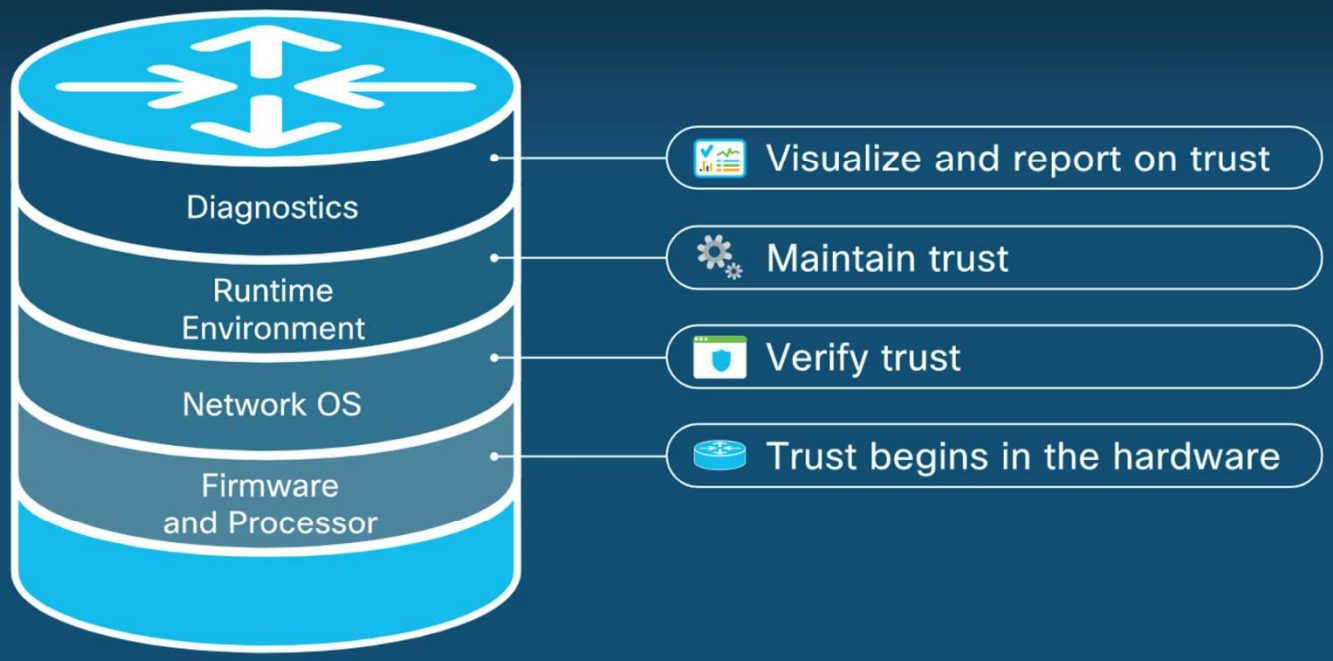
Why Hardware-Anchored Secure Boot Matters



https://blog.f-secure.com/cold-boot-attacks/

https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

Trusted Platform



Secure boot is a control.

Once it’s complete, how do you know it actually happened?

Would you trust a device to tell you it’s trusted?

Measuring and Validating Trust

Boot & Runtime Measurements

Known Good Values (KGV)

e5fa44f2b31c1fb553b46021e7360d07d5d91ff5e
7448d8798a4380162d4b56f9b452e2f6f9e24e7a
a3db5c13ff90a36963278c6a39e4ee3c22e2a436

e5fa44f2b31c1fb553b46021e7360d07d5d91ff5e
7448d8798a4380162d4b56f9b452e2f6f9e24e7a
a3db5c13ff90a36963278c6a39e4ee3c22e2a436

9c6b057a2b9d96a4067a749ee3b3b0158d390cf1
5d9474c0309b7ca09a182d888f73b37a8fe1362c

9c6b057a2b9d96a4067a749ee3b3b0158d390cf1
5d9474c0309b7ca09a182d888f73b37a8fe1362c

ccf271b7830882da1791852baeca1737fcbe4b90
d3964f9dad9f60363c81b688324d95b4ec7c8038

ccf271b7830882da1791852baeca1737fcbe4b90
d3964f9dad9f60363c81b688324d95b4ec7c8038

Note: Focus on Known-Good Values. This is not blacklisting.

Secure Quote Process

1) Service requests quote with unique nonce value

Integrity Verification Service

3) Service validates:

- Signature with enrolled key
- Nonce Value
- Measurements vs KGVs

e5fa44f2b31c1fb553b46021e7360d07d5d91ff5e
7448d8798a4380162d4b56f9b452e2f6f9e24e7a
a3db5c13ff90a36963278c6a39e4ee3c22e2a436
9c6b057a2b9d96a4067a749ee3b3b0158d390cf1
5d9474c0309b7ca09a182d888f73b37a8fe1362c
ccf271b7830882da1791852baeca1737fcbe4b90
d3964f9dad9f60363c81b688324d95b4ec7c8038
dd71038f3463f511ee7403dbcbc87195302d891c
4143d3a341877154d6e95211464e1df1015b74b
b6abd567fa79cbe0196d093a067271361dc6ca8b

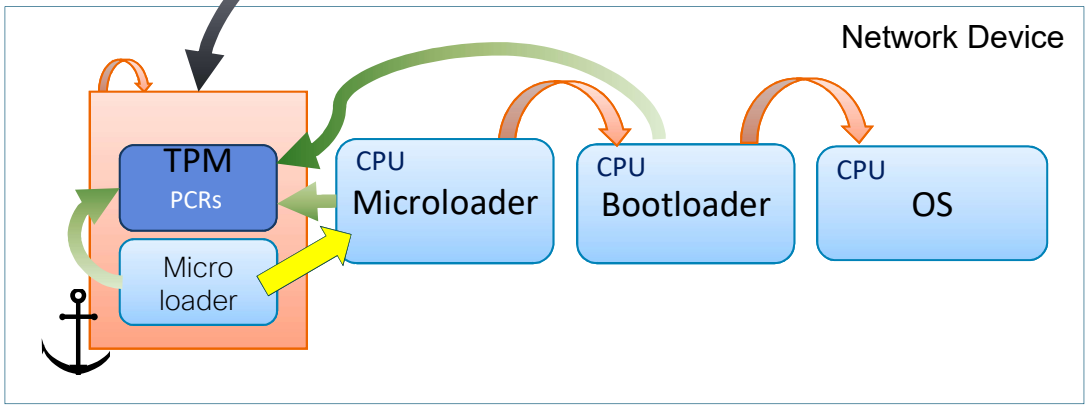
2) Router gathers measurements with nonce, creates attestation dossier within signed envelope

Boot Integrity Visibility

Securely measure: hardware, firmware, bootloader, and OS kernel at boot-time.

Integrity Verification

Remote Attestation



Must use external service to verify trust

Device Status	Device Name	IP Address	Trust Status
Reachable	4451-af08-6	10.122.83.63	Trusted
Reachable	4451-af08-7	10.122.81.32	Unknown
Reachable	4451-af08-9	10.122.81.36	Trusted
Reachable	asr1004-ag09-2	172.18.152.134	Unknown
Reachable	nd-ovld2	172.18.151.177	Unknown

Secure Boot signature check

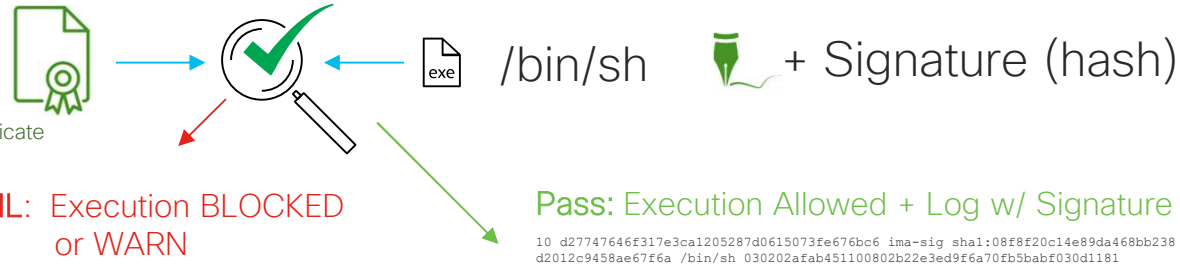
Integrity measurement

Extending Trust to Runtime: Process Integrity Validation

Logging


```
10 7103f91ed91be355abeef84853301e11dccd9e4a ima-sig
sha256:0b46fb8e7635a02320aceed326128b0f146c369476dfe5fd704aceca4a135b88 /bin/sh
```

Appraisal




```
10 d27747646f317e3ca1205287d0615073fe676bc6 ima-sig sha1:08f8f20c14e89da468bb238
d2012c9458ae67f6a /bin/sh 030202afab451100802b22e3ed9f6a70fb5babf030d1181
8152b493bd6bfd916005fad7fdcfd7f88d43f6cffaf6fd1ea3b75032dd702b661d4717729e4a3fa4
ee95a47f239955491fc8064eca8cb96302d305d59750ae4ffde0a5f615f910475eee72ae0306e4ae
0269d7d04af2a485898eec3286795d621e83b7dedc99f5019b7ee49b189f3ded0a2
```

PoC Demo: IOS XR Process Measurement

Process fingerprint reported by XR Kernel

```
RP/0/RP0/CPU0:xr9kv-imatest#run demo/imacheck
Sat Apr  7 01:43:53.356 UTC
10 025af7c31a792d974f6c2993c46852c62514e044 ima-sig sha256:58293675e57e7a023ed6702ebcd3b8b5ef496111962b9345e
e996c142fd266eb /misc/scratch/demo/malware-20180407-013759-test001
10 723ec40e5ff7cc48001f3d6bd295eb7e7197bf62 ima-sig sha256:988060966ee9e28cfd8647b33c21ab1e6846ea39905f4771f
f090c1fd28e6e6c /misc/scratch/demo/malware-20180407-013814-test002
10 a28cd0c726a5f63d757dd7c9f936bd53b76770b6 ima-sig sha256:091c1c6968e3d98ba5e94a4c6407d7d6ad5427c197ff763a3
2f9b1cacac6dcc1 /misc/scratch/demo/malware-20180407-013825-blue
10 a4758cffd077905919465fbc087a6044f6565b08 ima-sig sha256:2fa5fe8156de7eed21c5a380d31410894354245591a1f1c77
10b2c8f289db001 /misc/scratch/demo/malware-20180407-014345-testing003
```

(Demo) unauthorized processes identified

Hashes of all processes recorded by kernel

External Validation

Got Trust?

- External service to verify trust
- Collect and sign evidence
- Report and verify that it's accurate
- Understand the devices being reported on
- Evaluate the evidence versus "known good values"
- Provide insight into the trust posture of the device

Get Benefits

- Evidentiary trail
- Evidence with history
- Unique insights into production systems

IOS XR Trust:

Trusted Platform Technologies

Cisco Trust Anchor Module (TAm)

HW Root-of-trust and HW Security Module embedded in Cisco Devices

- Secure Boot HW Root
- Strong cryptographic engine
  - Secure Storage for Keys, Certificates, and Objects
- Unique Device Identity
- On each RP, LC, Fabric

Unique hardware Identity (SUDI)

- Unique cryptographic key embedded in hardware trust anchor module within every IOS XR Router
  - Secure Unique Device Identifier (SUDI)
  - Immutable key imbedded in Trust Anchor Module at time of manufacture
  - Signed by Cisco for proof of authenticity
  - Validates PID and Serial number of component
- Cryptographically strong identification of remote hardware
- Establishes unique, immutable hardware identity
- Can be used to sign authentication challenges & quotes

Secure Storage of Secrets

What is a secret?

IOS XR Secrets

- MACsec pre-shared keys
- SSH Host keys
- Private keys for TLS certificates
- User login password hashes
- Routing protocol authentication strings
- System protocol authentication strings (ntp, snmp, etc)

3rd Party Applications

- userID and passwords
- API keys
- TLS keys

Type 6 Encryption

Keys strongly encrypted within IOS XR Configuration

Step 1: Configure master key (AES)

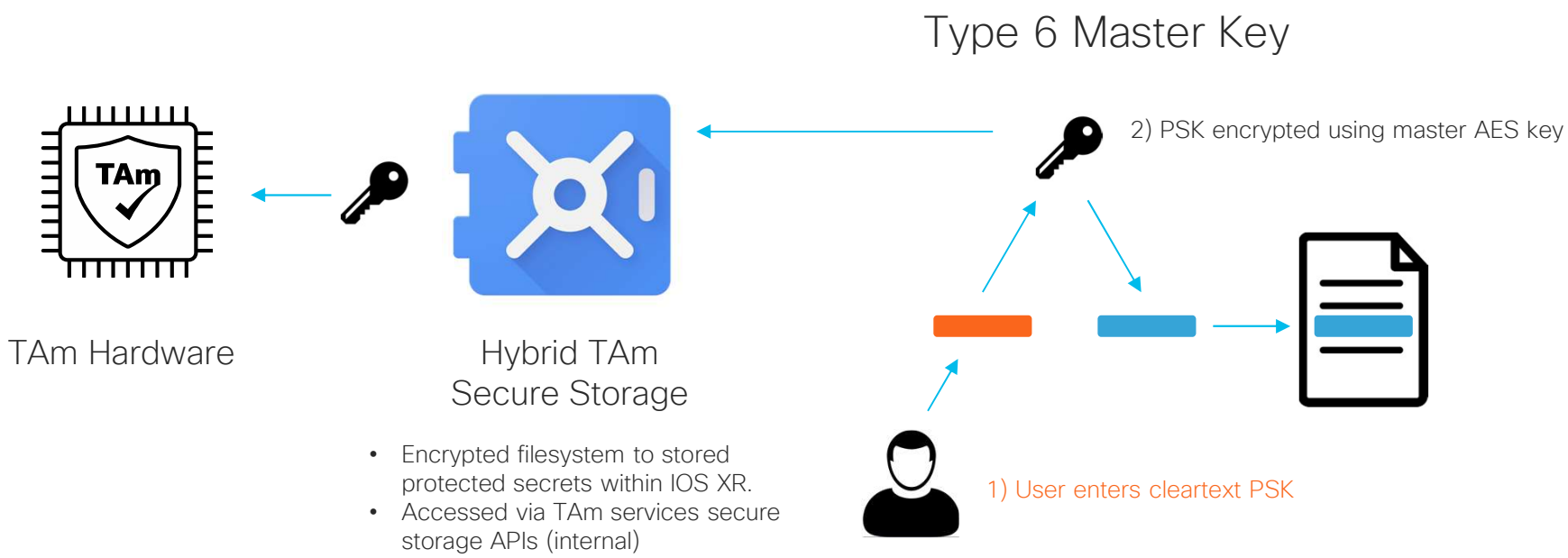
```
Router (config)# key config-key password-encrypt
New key: *******
Confirm key: ******
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys
with the new master keypas
Router (config)# key config-key password-encrypt
Old key: ******
New key: ******
Confirm key: Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

Type 6 service encrypts MACsec PSK Using AES cipher

```
Router# show running-config key chain kc1
key chain kc1
 macsec
   key 1111
     key-string password6
    5d63525a58594657565e68454468424659655548624 24c5
    95d696554694a424c59655f504a575e6648484c484b4646
    535d49675e535a60644e6045654a655f666858414142
      cryptographic-algorithm aes-128-cmac
        lifetime 00:00:00 january 01 2017 infinite
```

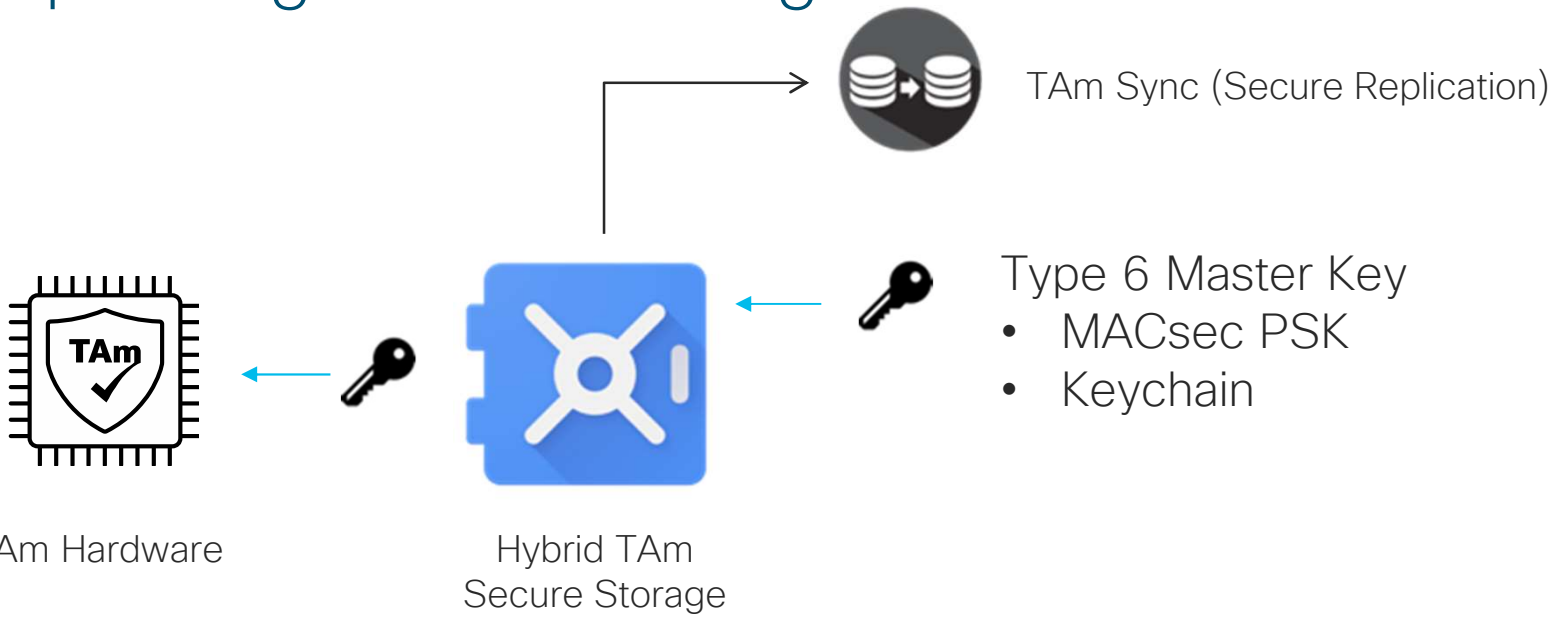
Master Key in TAm

Hardware Based Secure Storage



- Encrypted filesystem to stored protected secrets within IOS XR.
- Accessed via TAm services secure storage APIs (internal)

Expanding Secure Storage



- Encrypted filesystem to stored protected secrets within IOS XR.
- Accessed via TAm services secure storage APIs (internal)

Cisco Secure Development Lifecycle

Repeatable. Measurable. Resilient. Trustworthy.

Rigorous
evolving product security baseline

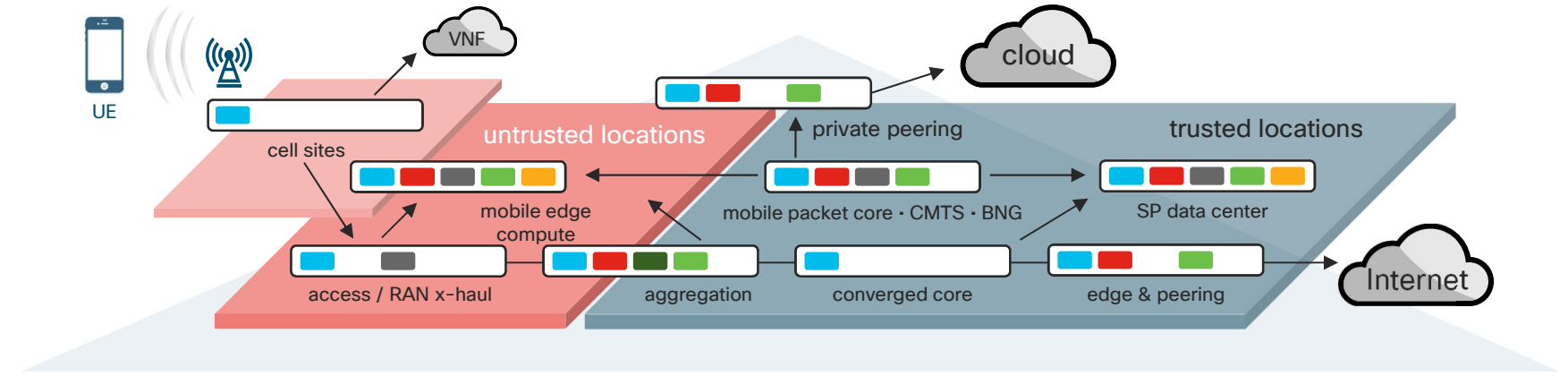
Minimizes
vulnerabilities, enhances security

Embeds
security across the portfolio

Trusted Platforms
Protocol and Platform Hardening
Security Services

Pervasive Security Strategy

IP infrastructure	subscriber services	automation	content & peering	SP services
network policy	subscriber id & policy	secure deployment	threat detection	anti-malware
network slicing	threat detection	audit & forensics	encrypted analytics	secure SD-WAN
infra protection	subscriber visibility	automated remediation	routing protection	zero-trust networking
traffic steering	content visibility	secure management	DDoS protection	SPM/API Security



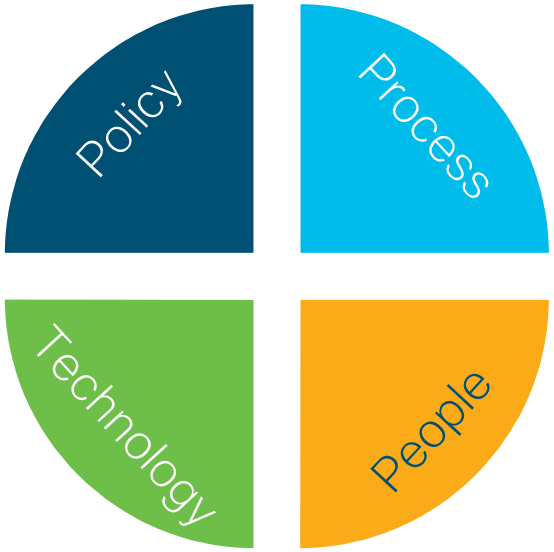
trusted network infrastructure & automation | critical & resilient infrastructure

trusted platforms

certified & compliant

Cisco's Multi-faceted Approach to Security

Trust & Pervasive Security



Key Takeaways on Trust

- Trusted Platforms requires a hardware root-of-trust
- Visibility and Reporting is critical to attest for the integrity of your Trusted infrastructure

Learn more @ trust.cisco.com
Visit cisco.com/go/sp-trust

take a photo

CISCO